EXHIBIT 3

Protect Your Computer From Viruses, Hackers, and Spies

oag.ca.gov/privacy/facts/online-privacy/protect-your-computer

Protect Yourself and Your Devices

Today we use internet-connected devices in all aspects of our lives. We go online to search for information, shop, bank, do homework, play games, and stay in touch with family and friends through social networking. As a result, our devices contain a wealth of personal information about us. This may include banking and other financial records, and medical information—information that we want to protect. If your devices are not protected, identity thieves and other fraudsters may be able to get access and steal your personal information. Spammers could use your computer as a "zombie drone" to send spam that looks like it came from you. Malicious viruses or spyware could be deposited on your computer, slowing it down or destroying files.

By using safety measures and good practices to protect your devices, you can protect your privacy and your family. The following tips are offered to help you lower your risk while you're online.

Keep your device secure

Make sure to download recommended updates from your device's manufacturer or operating system provider, especially for important software such as your internet browser. Antivirus software, antispyware software, and firewalls are also important tools to thwart attacks on

your device.

Keep up-to-date

Update your system, browser, and important apps regularly, taking advantage of automatic updating when it's available. These updates can eliminate software flaws that allow hackers to view your activity or steal information. Windows Update is a service offered by Microsoft. It will download and install software updates to the Microsoft Windows Operating System, Internet Explorer, Outlook Express, and will also deliver security updates to you. Patching can also be run automatically for other systems, such as Macintosh Operating System. For mobile devices, be sure to install Android or iPhone updates that are distributed automatically.

Antivirus software

Antivirus software protects your device from viruses that can destroy your data, slow down or crash your device, or allow spammers to send email through your account. Antivirus protection scans your files and your incoming email for viruses, and then deletes anything malicious. You must keep your antivirus software updated to cope with the latest "bugs" circulating the internet. Most antivirus software includes a feature to download updates automatically when you are online. In addition, make sure that the software is continually running and checking your system for viruses, especially if you are downloading files from the web or checking your email. Set your antivirus software to check for viruses every day. You should also give your system a thorough scan at least twice a month.

Antispyware software

Spyware is software installed without your knowledge or consent that can monitor your online activities and collect personal information while you're online. Some kinds of spyware, called keyloggers, record everything you key in—including your passwords and financial information. Signs that your device may be infected with spyware include a sudden flurry of ads, being taken to websites you don't want to go to, and generally slowed performance.

Spyware protection is included in some antivirus software programs. Check your antivirus software documentation for instructions on how to activate the spyware protection features. You can buy separate antispyware software programs. Keep your antispyware software updated and run it regularly.

To avoid spyware in the first place, download software only from sites you know and trust. Make sure apps you install on a mobile device come from the Apple App Store for iPhones or Google Play for Android devices.

Firewalls

A firewall is a software program or piece of hardware that blocks hackers from entering and using your computer. Hackers search the internet the way some telemarketers automatically dial random phone numbers. They send out pings (calls) to thousands of computers and wait for responses. Firewalls prevent your computer from responding to these random calls. A firewall blocks communications to and from sources you don't permit. This is especially important if you have a high-speed internet connection, like DSL or cable.

Some operating systems have built-in firewalls that may be shipped in the "off" mode. Be sure to turn your firewall on. To be effective, your firewall must be set up properly and updated regularly. Check your online "Help" feature for specific instructions.

Use strong protection

Making use of complex passwords and strong methods of authentication can help keep your personal information secure.

Choose strong passwords

Protect your devices and accounts from intruders by choosing passwords that are hard to guess. Use strong passwords with at least eight characters, a combination of letters, numbers and special characters. Don't use a word that can easily be found in a dictionary or any reference to personal information, such as a birthday. Some hackers use programs that can try every word in the dictionary, and can easily find personal information such as dates of birth. Try using a phrase to help you remember your password, using the first letter of each word in the phrase. For example, HmWc@w2—How much wood could a woodchuck chuck.

Choose unique passwords for each online account you use: financial institution, social media, or email. If you have too many passwords to remember, consider using password manager software, which can help you create strong individual passwords and keep them secure.

Use stronger authentication

Many social media, email, and financial accounts allow the use of stronger authentication methods. These methods can include using a fingerprint, one-time codes sent to a mobile device, or other features that ensure a user is supposed to have access to the account. For more information on strong authentication methods, visit the Lock Down Your Login Campaign.

Protect your private information

While checking email, visiting websites, posting to social media, or shopping, pay attention to where you click and who you give your information to. Unscrupulous websites or data thieves can attempt to trick you into giving them your personal data.

Be careful what you click

Phishing attacks—where hackers send seemingly genuine messages to trick you to hand over personal information—are becoming more sophisticated. For instance, you may receive an urgent message stating that your bank account has been locked and requiring you to enter your password and Social Security number to unlock it. Think twice before clicking on links in messages such as this. Most genuine messages from financial institutions will not ask for personal information directly, but will instead instruct you to call or visit a website directly. You can also verify the email address that sent the message to ensure it came from the expected sender.

Shop safely

When shopping online, check out the website before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, beware! Shop elsewhere.) Learn how to tell when a website is secure. Look for "https" in the address bar or an unbroken padlock icon at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers as it moves across the internet.

Be careful what you share

Social media allows sharing of all aspects of life, but it's important to control who has access to the information you share. Information thieves can use social media postings to gather information and then use the information to hack into other accounts or for identity theft. To protect yourself, make use of privacy settings to limit the visibility of personal posts to your personal networks, and restrict the amount of information you share with the general public.

Responding to data breaches

Even if you make all the right moves, your data may be stolen from a company you trusted to keep it safe. If you find that your personal information has been accessed without your authorization, take steps to protect yourself. Place a fraud alert on your credit file. Review your annual credit reports. And if you suspect your information has been breached, put a freeze on your credit file to prevent fraudsters from opening new accounts in your name. For more information, see the Attorney General's information sheets on identity theft.

Parents, take control

Don't let your children risk your family's privacy. Make sure they know how to use the internet safely. For younger children, install parental control software on devices that limits the websites kids can visit. To protect your children's future credit, consider setting up a credit freeze for your child. But remember: no software can substitute for parental supervision.

Additional Information

Consumer information from the California Department of Justice, available at www.oag.ca.gov/privacy.

OnGuard Online

Practical tips from the federal government and the technology industry to help you be on guard against internet fraud, secure your computer, and protect your personal information.

Online Guide to Practical Privacy Tools

Computer security resources from the non-profit Electronic Privacy Information Center.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.